REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
Aug 2010	Conference Paper (Post Print)	JUN 2007 – AUG 2010

4. TITLE AND SUBTITLE
MANAGING NETWORK SECURITY POLICIES IN TACTICAL MANET'S USING DRAMA

5a. CONTRACT NUMBER FA8750-07-C-0110
5b. GRANT NUMBER N/A
5c. PROGRAM ELEMENT NUMBER 62702F
5d. PROJECT NUMBER NATM
5e. TASK NUMBER TE
5f. WORK UNIT NUMBER LC

6. AUTHOR(S)
Yuu-Heng Cheng, Abhrajit Ghosh, Ritu Chadha, Gary M. Levin, Michelle Wolbert, C. Jason Chiang, Gregory Hadynski

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Telcordia Technologies Inc
One Telcordia Drive
Piscataway NJ 08854

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site/RITF
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TP-2012-008

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED: PA #: 88ABW-2010-4176
DATE CLEARED: 4 Aug 2010

13. SUPPLEMENTARY NOTES
© 2010 IEEE. Published in IEEE Conference proceeding for the 2010 Military Communications Conference – Cyber Security and Network Management Conference pp960-964, 31 Oct – 3 Nov 2010, San Jose CA. This work was funded in whole or in part by Department of the Air Force contract number FA8750-07-C-0110. This work is copyrighted. One or more of the authors is a U.S. Government employee working within the scope of their Government job; therefore, the U.S. Government is joint owner of the work and has the right to copy, distribute, and use the work. All other rights are reserved by the copyright owner.

14. ABSTRACT
Military networks are required to adapt their access control policies to the Information Operations Condition (INFOCON) levels to minimize the impact of potential malicious activities. Such adaptations must be automated to the extent possible, consistent with mission requirements, and applied network-wide. In this paper, we present a Policy-Based Network Security (PBNS) management approach for tactical MANETs. This approach leverages the DRAMA policy based network management system and the Smart Firewall system to meet the above requirement. It allows administrators to specify low-level network access control policies for each INFOCON level using high-level policies (adapted from the Smart Firewalls approach). The high-level policies are securely distributed to all the policy decision points in the network, which evaluate and enforce policies in a distributed manner. As a consequence of enforcing policies in response to INFOCON level changes, appropriate access control policies will be derived and applied to local firewall devices without human intervention. Thus, operator burden can be significantly reduced and inadvertent errors can be avoided.

15. SUBJECT TERMS
network access control; network operations; firewalls; MANET; security; policy-based management

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
U	U	U	UU	6	GREGORY HADYNSKI
					19b. TELEPHONE NUMBER (*Include area code*) N/A

Managing Network Security Policies in Tactical MANETs Using DRAMA

Yuu-Heng Cheng, Abhrajit Ghosh, Ritu Chadha,
Gary M. Levin, Michelle Wolberg, C. Jason Chiang
Knowledge-Based Systems, Telcordia
Piscataway, NJ, U.S.A.
chadha@research.telcordia.com

Gregory Hadynski
Air Force Research Laboratory
Rome, NY, U.S.A.
Gregory.Hadynski@rl.af.mil

Abstract—**Military networks are required to adapt their access control policies to the Information Operations Condition (INFOCON) levels to minimize the impact of potential malicious activities. Such adaptations must be automated to the extent possible, consistent with mission requirements, and applied network-wide. In this paper, we present a Policy-Based Network Security (PBNS) management approach for tactical MANETs. This approach leverages the DRAMA policy based network management system and the Smart Firewall system to meet the above requirement. It allows administrators to specify low-level network access control policies for each INFOCON level using high-level policies (adapted from the Smart Firewalls approach). The high-level policies are securely distributed to all the policy decision points in the network, which evaluate and enforce policies in a distributed manner. As a consequence of enforcing policies in response to INFOCON level changes, appropriate access control policies will be derived and applied to local firewall devices without human intervention. Thus, operator burden can be significantly reduced and inadvertent errors can be avoided.**

Keywords: network access control; network operations; firewalls; MANET; security; policy-based management;

I. INTRODUCTION

The dynamic nature of tactical MANETs (*Mobile Ad-hoc Networks*) makes it hard to manually manage their operations in a consistent manner across all network elements. Tactical MANETs must conform to war fighter requirements and at the same time adapt to changing network conditions such as intermittent connectivity. Security concerns within such MANETs are significant owing to the fact that network nodes are often vulnerable to capture and compromise. While *Intrusion Detection Systems* (IDSs) are able to detect potential threats, *Information Assurance* (IA) operations that mitigate these threats are usually left to the network operators. As in the case of other network management activities in MANETs, IA goals are difficult to achieve, especially if done using manual means. Changing network configurations in response to changing threat levels, if done manually, can be cumbersome and error prone. There is thus a need to automatically adapt IA operations, in response to changing threat levels, with minimal human intervention. This will ensure timely and correct adaptations to network threats.

Policy based management is a promising approach for automating threat level based adaptation of IA activities in a network. Policy based IA is a major research area at *Defense Advanced Research Projects* Agency (DARPA [7]). Continuous and active efforts in this area have produced systems such as [3], [4], [6], and [8]. The systems described in [4] and [8] provide and validate abstract models of access control lists (ACLs) and provide methods to support their management. However, these systems are not designed to automatically react to changes in network threat levels as described for example, by the *Information Operations Condition* (INFOCON [10]) system. The effort in [3] defined requirements for high-security MANETs and described selected aspects of their implementation. The authors addressed prevention of outsider and insider attacks using policy-based network management. However, the paper did not have additional information on how to apply such a system in a military environment. The authors in [6] describe a hardware implementation of a distributed security architecture without clarifying the details of the system to be used to manage the architectural components.

In this paper, we describe an approach to Policy Based Network Security (PBNS) management for wireless ad hoc networks. The PBNS capability described in this paper is an extension of *Dynamic Re-Addressing and Management for the Army* (DRAMA [2]), a system for policy based network management. The extended system enables administrators to a) define network security policies for a MANET based on INFOCON levels, b) protect DRAMA agents from malicious node activities by leveraging input from Intrusion Detection Systems (IDSs), and c) secure the policy distribution process itself. Additionally, the design addresses some of the lessons learned in [7].

In Section II, we describe the concerns that motivate the securing of MANET communication as well as the network management process. In Section III, we describe the architecture and implementation of PBNS functionalities and

The research reported in this document/presentation was performed in connection with contract number FA8750-07-C-0110 with the U.S. Air Force Research Laboratory. The views and conclusions contained in this document are those of the authors and should not be interpreted as presenting the official policies or position, either expressed or implied, of the U.S. Air Force Research Laboratory, or the U.S. Government unless so designated by other authorized documents. Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

Approved for Public Release; Distribution Unlimited: 88ABW-2010-4176 dated 4 August 2010.

978-1-4244-8180-4/10/$26.00 ©2010 IEEE 960

provide some performance results collected from our experiments using the implementation. Section IV summarizes our contributions and presents the directions for future work.

II. Network Management Security Concerns

DRAMA is a policy-based management system for wireless ad hoc networks which was demonstrated in an outdoor environment at Fort Dix, New Jersey in 2005 and was assessed at TRL-6. DRAMA policy agents run on nodes within the network and collaboratively manage the MANET as a whole. At the highest level, the Global Policy Agent (GPA) manages multiple Domain Policy Agents (DPAs). A DPA can manage multiple DPAs or Local Policy Agents (LPAs). An example DRAMA hierarchy is depicted in Figure 1. Each policy agent performs local policy-controlled configuration, monitoring, filtering, aggregation, and reporting of network management data. Policies, a set of rules for network management, are disseminated from the GPA to DPAs and then to LPAs. Policy controlled configuration changes are enforced using software modules referred to as *DRAMA Actions*. Actions can be created within the DRAMA framework by following the DRAMA programming guidelines. A set of standard network management actions is delivered with DRAMA. In this architecture, any node can dynamically take over the functionality of another node to ensure survivability. Since each policy agent is able to make local decisions, only aggregated information is delivered through the hierarchy. Every node in the network has an identical set of active policies to ensure consistent behavior in the MANET. The separation of policy enforcement and policy content reduces network management bandwidth overhead. On the other hand, ensuring that correct and non-tampered policies contents are distributed to each policy agent is very important.

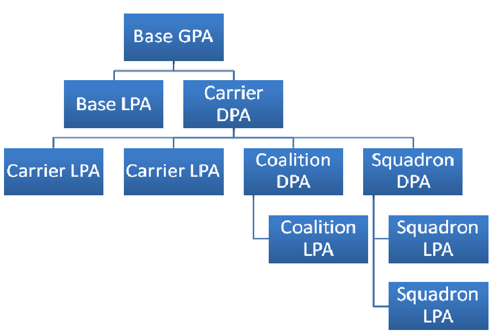

Figure 1. DRAMA hierarchy for the example network

The DRAMA network hierarchy may or may not directly reflect the physical topology of a network. The hierarchy may be physically connected as illustrated in Figure 2. In this example, there are four network management domains: Base, Carrier, Squadron, and Coalition. Streaming and web services are provided on different nodes as denoted in the figure. All wireless communication is assumed to be encrypted to ensure confidentiality.

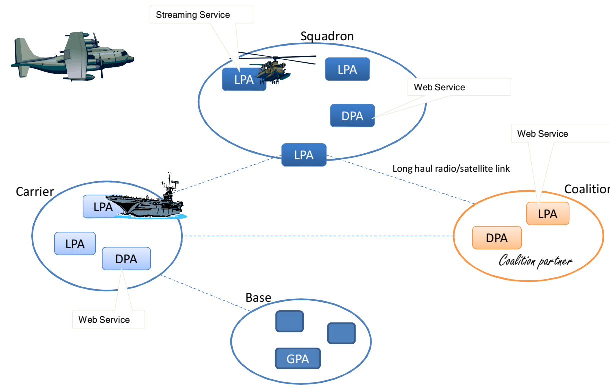

Figure 2. Physical topology of a network

Table 1 lists a brief summary of the network threat environment associated with each INFOCON level and the associated mitigation procedures. When the INFOCON level changes, *Access Control Lists* (ACLs) on each node may need to be modified. Manual configuration of each node may not be trivial and may be prone to error. Several existing management and analysis tools (e.g., [4] and [9]) can facilitate automated ACL configuration. These tools allow administrators to configure ACLs via high level abstractions of the network. The PBNS capability leverages such a tool [4].

Table 1: INFOCON levels

INFOCON	Summary
Level 5	A situation where there is no apparent hostile activity against computer networks.
Level 4	A situation where increased monitoring of all network activities is mandated.
Level 3	A situation where a risk has been identified.
Level 2	A situation where non-essential networks may be taken off-line, and alternate methods of communication may be implemented.
Level 1	A situation when attacks are taking place and the Computer Network Defense system is at maximum alertness

The automated configuration of ACLs based on INFOCON level enables the MANET to rapidly react to changes in the tactical network. For network attack detection, we rely on information from existing *Intrusion Detection Systems* (e.g., NIDS [8]). This intelligence is incorporated into the DRAMA system as *Intrusion Detection Message Exchange Format* (i.e. IDMEF [5]) messages. When an intrusion is detected, manual reconfiguration prolongs the response to INFOCON level change. The PBNS uses IDMEF notifications to trigger DRAMA actions and thereby ensures that proper network configurations are applied in a timely manner.

III. POLICY BASED NETWORK SECURITY

A. System Architecture

DRAMA provides a flexible agent-based infrastructure that allows dynamic insertion of new management functionality. We leverage this infrastructure to incorporate PBNS functionalities as illustrated in Figure 3.

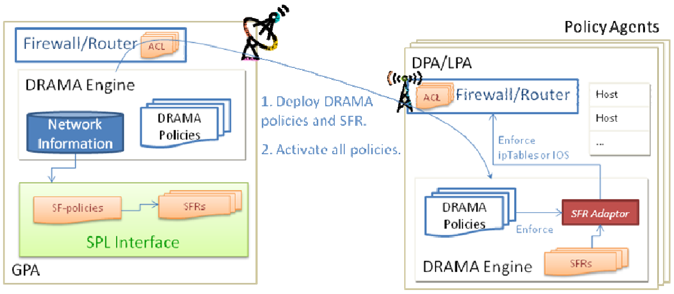

Figure 3. PBNS architecture in DRAMA

Each policy agent (GPA, DPA, or LPA) consists of a firewall/router, a DRAMA engine and optionally several hosts or devices that are managed by the DRAMA engine. The policy agents typically communicate over a wireless network. The GPA provides a console for network administrators to remotely determine the active policy set for all agents in the MANET.

We introduce a new component called the *Security Policy Language* (SPL) interface. The SPL interface runs on the GPA and may be used by a network administrator to specify high level network access control policies, which we refer to as *Smart Firewall policies* (a.k.a., SF-policies). SF-policies, which are described later in this section, are used to construct DRAMA policies that pertain to network access control rules. These SF-policies are then translated into vendor independent access control rule sets (a.k.a. *Smart Firewall Rules*, SFRs) for each policy agent in the network. These SFRs are then delivered to each platform where they are translated into device specific access control lists such as iptables [1] rules or Cisco IOS [11] commands. The current implementation supports translation to iptables rules only. The SFRs are transmitted to all the policy agents via a secure transport.

All DRAMA policies, including the ones that pertain to network access control, are transmitted via the updated secure policy distribution mechanism described later in this section. Another new component, the SFR Adaptor, translates SFRs into device specific access control rules. It includes a DRAMA action that enforces the rules on the local platform firewall when DRAMA policies are triggered.

B. Security Policy Lanaguage

We reuse the implementation from [4] and adopt the SPL concept to provide a single interface for managing network access control lists for heterogeneous devices such as firewalls, routers, switches, and hosts. A security policy is a collection of access control rules that allow network administrators to define the access privileges under a specific INFOCON level. Table 2 lists three security policies that can be applied to our example network. By default all firewalls are configured to deny all services to assure information security [3]. The first security policy "NetOp-for-all" allows the different management domains to access the streaming and web services. The security policy "NetOp-USAF" allows only US air force to access the streaming and web services. The "No-Streaming" policy indicates that only web services accesses are allowed.

Table 2: Security policy examples

Name	High Level ACL
NetOp-for-all	*Allow Streaming* from Base, Carrier, Coalition to Squadron *Allow Web* from Base, Squadron, Coalition to Carrier *Allow Web* from Base, Coalition, Carrier to Squadron
NetOp-USAF	*Allow Streaming* from Base, Carrier to Squadron *Allow Web* from Base, Squadron to Carrier
No-Streaming	*Allow Web* from Base, Squadron to Carrier [Implies: Deny Streaming from ANY to Squadron]

These high level policies are then translated into the vendor independent SFR format. The PBNS functionality on each policy agent will then translate the SFR into corresponding device configurations. A summary of the translation flow is depicted in Figure 4.

Figure 4. Security policy translations

On the GPA, we define several DRAMA policies (as listed in Table 3) to apply different SFRs at different INFOCON levels based on the INFOCON level requirements described earlier in Table 1. Policy1 indicates that for INFOCON level 4 and 5, apply the SFR named "NetOp-for-all". When INFOCON is level 3 as matched in the condition for Policy2, then apply the SFR named "NetOP-USAF" and start monitoring the coalition DPA activity. Policy 3 applies the SFR named "No-Streaming" when INFOCON is in level 1 or 2. With these policies in place, DRAMA policy agents will be able to apply the corresponding SFR based on the local INFOCON level.

Table 3: DRAMA policy examples

Name	DRAMA Policy
Policy1	INFOCON > 3, Apply_SFR(NetOp-for-all)
Policy2	INFOCON == 3, Apply_SFR(NetOp-USAF) and Monitor_Traffic(Coalition_DPA)
Policy3	INFOCON < 3, Apply_SFR(No-Streaming)

C. *Secure Policy Language Interface*

The SPL interface combines network information, service definitions and security policies into SFRs as illustrated in Figure 5. Network information contains information on the logical management domains and on the physical devices (hosts). Physical device information includes IP addresses of interfaces and services that the device provides in details. This information can be obtained from the existing DRAMA system. The service definition allows the administrator to "name" a network communication protocol. This facilitates the expression of SF policy. The SF-policies are defined in XML format.

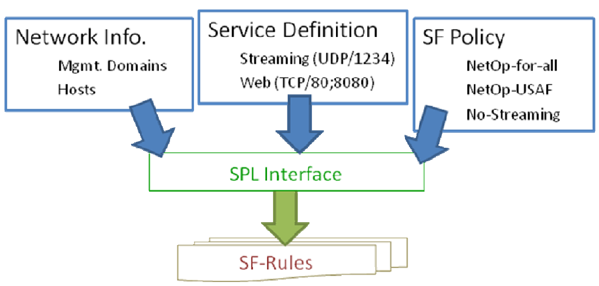

Figure 5. SPL interface

The SPL interface combines the network information, service definition, and a SF-policy into a set of SFR. Details can be found in [4].

D. *Interworking with Intrusion Detection System*

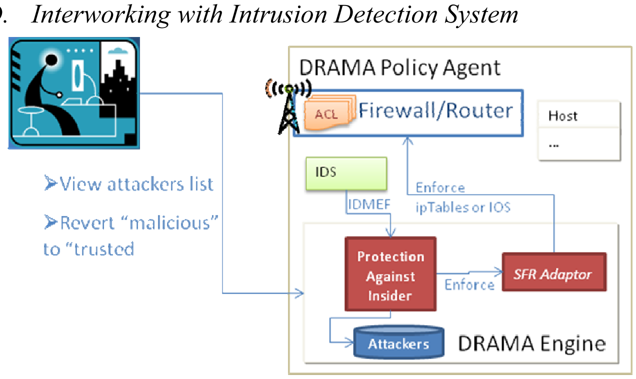

Figure 6. Interworking with intrusion detection system.

We assume an IDS can provide notification messages in the Intrusion Detection Message Exchange Format (i.e. IDMEF [5]). From this information, a policy agent is able to classify a remote policy agent as "trusted" or "malicious." An abstraction of the integration architecture is depicted in Figure 6. The *Protection Against Insider* (PAI) component receives the IDMEF messages. The information of a "malicious" node and the corresponding timestamp is stored in the *Attackers* repository. By default all nodes are considered as trusted unless notified otherwise by the IDS. When a remote policy agent is considered "malicious", the PAI component will trigger the SFR Adaptor to enforce a firewall configuration that drops all packets from the "malicious" node. This operation will be performed immediately by the DRAMA policy agents. The assumption is that the IDS is trustworthy. In addition, the PAI component will send an event to the local DRAMA engine. The DRAMA system allows the network administrator to manually revert the status of a node from "malicious" to "trusted". This process can be done only manually to defend against possible security breaches in PBNS.

E. *Secure Policy Distribution*

The security of a distributed architecture strongly relies on the security of information transmission. For over-the-air communications, in addition to the transport being encrypted, the transmitted content needs to be authenticated. These security concerns and basic architecture design were addressed in [3].

In the DRAMA system, all policies are intended to be created at and distributed from the GPA. To avoid man-in-the-middle attacks, where a compromised node injects policy operations as if they were issued by the GPA, policy operations are signed by the GPA. Nodes receiving policy operations always verify the signature to confirm message authenticity. Each operation uses a monotonically increasing sequence number to guarantee its uniqueness. The sequence number is part of the data being signed to defend against replay attacks. A compromised node cannot replay earlier operations and cause the installed policies to revert to an earlier set of policies. Note that once a remote node is identified as "malicious" by IDS, the communications to the remote node must be cut-off. This authentication, authorization, and replay protection is intended to protect DRAMA from attacks that occur before the IDS had detected the problem. Details of the protocol exchange mechanism are provided in [12].

The DRAMA system further ensures secure policy-based management of network resources by providing authentication services for distributed policies. All the DRAMA policies are signed with the GPA's private key and then distributed to other nodes in the DRAMA management hierarchy. The recipients of these policies will validate the content by using the GPA's public key. If the validation failed, the policy content will not be accepted. This authentication will prevent malicious nodes from attacking the DRAMA management system with spoofed policy updates.

F. *Implementation Performance*

The implementation of the PBNS extension discussed in this paper, except for the secure policy distribution, was tested and demonstrated on a 10-node virtual airborne network over the VAN testbed [13]. The virtual network was based on the network setup shown in Figure 2. The security policies, NetOp-for-all, NetOp-USAF, and No-Streaming were converted to SFRs and delivered to all nodes prior to the mission. The

average size of a zipped SFR is about 8Kbytes. The SFRs were then translated into iptables rules by the SFR Adaptor. The DRAMA policy agent was loaded with the policies listed in Table 3. A GUI interface was used to disseminate INFOCON level change events from the GPA to all nodes. One key performance metric that was measured was the system response time for applying a security policy. The event dissemination time depends on the network condition and is not discussed here. With the SFRs in place, on average a DRAMA node takes 405ms to apply the iptables rules after a DRAMA policy is triggered.

We used a simple IDS-surrogate to publish an IDS_NOTIFICATION trigger event to notify the PAI component about the detection of a malicious node. It took 330ms on average for a DRAMA node to block the malicious node.

IV. Summary and Future Work

DRAMA is a distributed network management system. In this paper we described the addition of a network access control feature that can adapt to the current INFOCON level. This was done by integrating SPL and IDMEF notification processing into the DRAMA system. We increase the communication security via signing payloads to provide authorization and replay protection.

Potential future work includes

- Use of the SPL interface to support "what-if" scenarios. Provide a user interface for network administrators to evaluate the impacts of a SF-policy before deployment [7].
- Integrate with operational IDS. Technically, any system that supports IDMEF notifications can be integrated.

Acknowledgment

We are grateful to Shih-Wei Li for his comments and help in completing this work.

References

[1] O. Andreasson. Iptables Tutorial, 2006. [Online]. Available: http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html. [Accessed: March 31, 2010].

[2] R. Chadha, Y.-H. Cheng, J. Chiang, G. Levin, S.-W. Li, A Poylisher, "Policy-based Mobile Ad Hoc Network Management for DRAMA", in Proceedings of MILCOM 2004.

[3] Y.-H. Cheng, M. Raykova, A. Poylisher, S. Alexander, M. Eiger, S. M. Bellovin, "The Zodiac Policy Subsystem: A Policy-Based Management System for a High-Security MANET," Policies for Distributed Systems and Networks, IEEE International Workshop on, pp. 174-177, 2009 IEEE International Symposium on Policies for Distributed Systems and Networks, 2009.

[4] J. Burns, et al., "Automatic management of network security policy," in Proceedings of DARPA Information Survivability Conference and Exposition II (DISCEX '01), volume 2, Anaheim, California, June 2001.

[5] H. Debar, D. Curry, and B. Feinstein, "The Intrusion Detection Message Exchange Format (IDMEF)," RFC 4765.

[6] T. K. Ramesh, J. L. Meier, J. E. Amanatullah, M. Huang, "Distributed security architecture," U.S. Patent Application US 2009/0228951, Sep. 10,2009.

[7] R. E. Smith, "Experiementing with Security Policy," in Proceedings of DARPA Information Survivability Conference & Exposition II (DISCEX '01), volume 1, pp. 116 -122, 2001.

[8] T. E. Uribe and S. Cheung, "Automatic Analysis of Firewall and Network Intrusion Detection System Configurations," in Journal of Computer Security, vol. 15, no. 6, pp. 691-716 , 2007.

[9] L. Yuan, H. Chen, J. Mai, C.-N. Chuah, Z. Su, P. Mohapatra, "FIREMAN: a toolkit for firewall modeling and analysis," in IEEE Symposium on Security and Privacy, pp. 198-213, May 2006.

[10] Strategic Command Directive (SD) 527-1, "Department of Defense Information Operations Condition (INFOCON) System Procedures," January 27, 2006. [Online]. Available: http://publicintelligence.net/strategic-command-directive-sd-527-1/. [Accessed: March 29, 2010].

[11] Cisco Systems Inc. (2010, Apr.) Cisco IOS and NX-OS Software. [Online]. http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html

[12] R. Chadha et al., "Policy-Based Mobile Ad Hoc Network Management", Proceedings of the IEEE 5th International Workshop on Policies for Distributed Systems and Networks, Yorktown Heights, New York, June 7-9, 2004.

[13] P. K. Biswas et al., "An integrated testbed for Virtual Ad Hoc Networks," Testbeds and Research Infrastructures for the Development of Networks & Communities, International Conference on, pp. 1-10, 2009 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops, 2009.